Workshop on Biometrics and E-Authentication Over Open Networks

Ms. Jeanette Thornton

Office of Management and Budget

E-GOV

US Internet Usage

- **Internet Usage increasing:** About 66% of American adults go online. (133 million people).
- **Use of online Banking:** 44% of internet users and 25% of all adults use online banking.
- **A lot of Government Paperwork:** Over 4,000 forms online

Source: Pew Internet and American Life Project, www.pewinternet.org

Policy: Not All E-Gov Is the Same

OMB Policy:
Establishes 4 Levels
E-Authentication
Guidance for Federal Agencies

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity (e.g. self identified user/password)	Some confidence in asserted identity (e.g. PIN/Password)	High confidence in asserted identity (e.g. digital cert)	Very high confidence in the asserted identity (e.g. Smart Card)

NIST SP800-63
Technical Guidance on
Electronic Authentication

The Need: E☆Authentication

- Enable millions of safe, secure, trusted online transactions between Government and the citizens and businesses that it serves
- Reduce online identity management / credentialing burden for government agency application owners and system administrators
- Provide citizens and businesses with a choice of credentials when accessing public-facing online government agency applications

Use of Federated Identity is Growing

- More than 300 businesses deploying SAML-based federations this year
  - Boeing (Airline mechanics and ground service personnel)
  - General Motors (500,000 employees, customers and trading partners)
  - Fidelity Investments (Employees and plan administrators from over 11,000 companies)
  - SAFE-BioPharma

Source: Burton Group

HSPD-12 Overview

- Common ID Standard for Federal Employees and contactors
- All Federal Employees/Contractors will posses a token with biometric
- ID is trusted across government
- Need to ensure privacy is protected

Implementation Schedule

Date	Deliverable
2-25-05	Final standard released
6-27-05	Agencies have completed implementation plan
10-27-05	You must use IDs meeting the standard to access facilities and info systems.

What is the role of biometrics?

- Can it be implemented over open networks? Limited to closed networks?
- Must it remain token based?
- Can it be used in a Federated Environment?
- What types of transactions? What levels?
- How will the public respond? Optional/mandatory

Other Possibilities

- Use of Biometrics for tele-work situations
- Limit NIST guidance to Federations of Closed communities
  - Federal employees/contractors
  - Medical
- Movement of Government to shared service providers for PKI/Smart Cards